

IN THE CLAIMS:

1-37. (cancelled)

38. (currently amended) A method to protect from unauthorized access electronic data objects, each electronic data object being related to a particular medical patient, comprising the steps of:

providing a separate application data store containing said patient related electronic data objects, said data objects comprising in addition to a name of the respective patient one of the additional information types selected from a group consisting of at least laboratory reports, study results, diagnostic findings and billing data of the respective medical patient, each electronic data object having an associated data object identifier which is automatically generated using information stored in the data object so that the identifier is dependent on the content of the data object and wherein the data object identifiers themselves carry information in addition to said patient name about a content of the respective data objects comprising at least one of said additional information types selected from said group consisting of said laboratory reports, study results, diagnostic findings, and billing data of the respective medical patient so that the data objects are systematically classified and arranged for association with access right categories to form structural connections of the data object to groups, teams, or references to people;

providing a separate user group store for association of a plurality of unique medical field user IDs dependent on previously determined information for identification and authentication of the medical field users;

providing a separate data object category store for said association of said data object identifiers with said access right categories so that access rights can thereby be determined from the data object itself;

providing a separate access right store for associating said medical field user IDs with said access right categories so that it can be determined for a particular medical field user the type of access allowed for the particular medical field user for reading, changing, or deleting information contained in the data objects;

providing an access control module connected to access said access right store, said data object category store, and said user group store and which monitors and controls data accesses by said medical field users to said data objects in said data application store, said access control module determining a medical field user ID from the user group store, and using said medical field user ID, determining an access right category via said access right store, and via access to said data object category store, said access control module determining, using said data object identifiers, which access right category is associated with the data object which the medical field user is attempting to access.